Amendments to the Specification:

Please replace paragraph [0011] of the specification with the following amended paragraph:

In a preferred embodiment, the claimed invention provides a method for automatically updating a ciphering key used in a network system. The network system comprises a server, an access point connected to the server, a station, and a counting module. The access point is used to transmit data received from the server via wireless transmission, and receive data transmitted via wireless transmission. The access point uses a first ciphering key to encrypt transmission data. The station is used to receive data transmitted from the access point via wireless transmission, and transmit data to the access point via wireless transmission. The station stores the first ciphering key for encrypting data transmitted to the access point. The counting module is installed in the server, the access point, or the station, for counting a time. The method comprises: ~~detonating~~ activating the counting module to start counting the time; randomly generating a second ciphering key if the time counted by the counting module conforms to a predetermined time; the access point transmitting the second ciphering key to the station so as to update the first ciphering key stored in the station with the second ciphering key; and using the second ciphering key to encrypt data transmitted between the access point and the station.

Please replace paragraph [0017] of the specification with the following amended paragraph:

Please refer to Fig.2. Fig.2 is a structural diagram of a present invention wireless network system 30. The wireless network system 30 comprises a server 32, at least an access point 34, and a plurality of stations P1, P2, P3. The access point 34 and the stations P1, P2, P3 all store an identical first ciphering key K1. Each station P1, P2, P3 stores an individual identification data I1, I2, I3. The server 32 stores a registration data I corresponding to the identification data I1, I2, I3 so as to control data access of the stations P1, P2, P3. The difference between the present invention wireless network system 30 and the prior art wireless network system 10 is that the server 32 of the present invention wireless network system 30 further comprises a counting module 36, and the access point 34 further comprises a random-code generation program 38. The counting module 36 is used to count a real time. When the time counted by the counting module 36 conforms a predetermined time, the counting module 36 sends a signal to the access point 34 to ~~detonate~~ activate the random-code generation program 38 to generate a new second ciphering key K2. Then, the server 32 controls the stations P1, P2, P3 and the access point 34 to update the first ciphering key K1 into the second ciphering key K2. The update method is illustrated as follows.

Please replace paragraph [0020] of the specification with the following amended paragraph:

~~Detonate~~ Activate the counting module 36 inside the server 32 to start counting the time;

Please replace paragraph [0021] of the specification with the following amended paragraph:

If the time counting by the counting module 36 conforms the predetermined time, the counting module 36 sends a signal to the access point 34 to ~~detonate~~ activate the random-code generation program 38 inside the access point 34 to randomly generate a second ciphering key K2;

Please replace paragraph [0053] of the specification with the following amended paragraph:

The first ciphering key K1 is successfully updated into the second ciphering key K2, the access point 34 and the station P1 use the second ciphering key K2 to encrypt or decrypt the transmission data until the next time that the counting module 36 ~~detonates~~ activates the random-code generation program 38 to generate a third ciphering key K3, then repeat the above steps to update the second ciphering key K2 into the third ciphering key K3, therefore, the common ciphering key inside the wireless network system 30 is changed unceasingly, the common ciphering key and the transmission data inside the wireless network system 30 can be kept secret.

Please replace paragraph [0054] of the specification with the following amended paragraph:

The counting module 36 of the embodiment mentioned above is installed inside the server 32, and the random-code generation program 38 is stored inside the access point 34. However, the present invention is not limited in that. The present invention counting module 36 can also be installed inside the access point 34. The random-code generation program 38 also can be stored inside the server 32. As long as the random-code generation program 38 is ~~detonated~~ activates to generate a new ciphering key each time the counting module 36 conforms to a predetermined time, it is covered by the disclosure of the present invention. In addition, the predetermined time can be a fixed time or a non-fixed time. That means the wireless network system 30 can update the common ciphering key according to a fixed time or a random time. No matter if the common ciphering key is updated according to a fixed time or a random time, the ciphering key also can be automatically updated.

Please replace paragraph [0056] of the specification with the following amended paragraph:

In contrast to the prior art method, the present invention method ~~detonates~~ activates the random-code generation program 38 to generate a new ciphering key each time the time counted by the counting module 36 conforms to a predetermined time. Then the old ciphering key stored inside the access point 34 and each station P1, P2, P3 is updated into the new ciphering key. Therefore, the network operators do not need to spend time and manpower to manually change the old ciphering key into the new ciphering key one by one. Moreover, since the ciphering key is generated by the random-code generation program, none of the network operators and the users of the stations know the content of the new ciphering key. Thus, the ciphering key can truly be kept secret. In addition, the ciphering key is updated randomly and frequently, thereby preventing network hackers from breaking into the wireless network system 30. Therefore, users that use the present invention method can not only enjoy the convenience of data transmission, but also can keep the transmitted data secret.

Please replace the abstract of the invention with the following amended paragraph:

A method for automatically updating a ciphering key used in a network system. The network system has a server, an access point connected to the server, a station, and a counting module. The access point is used to transmit data received from the server via wireless transmission, and receive data transmitted via wireless transmission. The access point uses a first ciphering key to encrypt transmission data. The method includes: ~~detonating~~ activating the counting module to start counting the time; randomly generating a second ciphering key if the time counted by the counting module conforms to a predetermined time; the access point transmitting the second ciphering key to the station so as to update the first ciphering key stored in the station with the second ciphering key; and using the second ciphering key to encrypt data transmitted between the access point and the station.